GUARDIAN 360°

QUICKSCAN BENCHMARK

Rapport de benchmark sécurité web

Pays-Bas · Belgique · Allemagne · France · autres pays

Édition août 2026

Basé sur 12 914 domaines analysés

Table des matières

1. Synthèse

Ce rapport de benchmark dresse le niveau de sécurité de sites web publics à partir du Guardian360 Quickscan. Pour cette édition, 12 914 domaines ont été analysés avec succès. Le Quickscan évalue notamment la présence des en-têtes de sécurité essentiels, les erreurs de configuration courantes, la Content Security Policy, le paramétrage SPF dans le DNS et la qualité de la configuration SSL/TLS. Chaque domaine reçoit un score de 0 à 100.

Le score moyen sur l'ensemble des domaines s'établit à 68,6 points, sur une échelle plafonnée à 100 points. Cela indique un niveau de base correct, mais aussi des retards structurels sur plusieurs mesures de sécurité importantes. Les mesures modernes et préventives, comme une Content Security Policy et des configurations SSL/TLS strictes, accusent un retard massif.

Des différences nettes apparaissent entre les quatre marchés clés de Guardian360. **La Belgique** obtient le meilleur score avec une moyenne de 72,7 et présente le moins de vulnérabilités sur presque tous les thèmes. **Les Pays-Bas** et **l'Allemagne** se situent près de la moyenne, à 68,9 et 68,4 respectivement. **La France** reste en retrait à 64,3 et affiche les taux de vulnérabilité les plus élevés sur la plupart des en-têtes.

Les principaux constats en résumé :

- Les en-têtes de sécurité manquants sont la règle plutôt que l'exception. Sur environ 60% des domaines, un en-tête X-Frame-Options est absent et sur près de la moitié une configuration HSTS correcte fait défaut.
- Une Content Security Policy est absente sur 73,2% des domaines. C'est la lacune la plus fréquente, tous pays confondus.
- Trois quarts des domaines (75,6%) présentent au moins une vulnérabilité dans la configuration SSL/TLS, comme des protocoles obsolètes ou des chiffrements faibles.
- Les mesures de base sont en revanche largement en ordre. Les erreurs de configuration graves, comme une page PHPinfo exposée (1,6%) ou une méthode HTTP TRACE active (0,9%), sont rares.

Le message est clair. La plupart des organisations maîtrisent les fondamentaux, mais laissent de côté des gains de sécurité simples à obtenir et à forte valeur, sur les en-têtes, la CSP et le durcissement TLS. C'est précisément là que le Quickscan offre un point de départ concret et mesurable pour progresser.

2. À propos de ce benchmark

2.1 Objectif

Avec le Quickscan, Guardian360 réalise une analyse de sécurité automatisée et non intrusive de la partie publiquement accessible d'un site web. Ce benchmark agrège les résultats d'un grand nombre d'analyses en une vue de marché. L'objectif est de donner aux distributeurs, partenaires et clients une idée de la position du niveau de sécurité d'un domaine par rapport au marché et à des organisations comparables dans d'autres pays.

Vous souhaitez savoir comment votre propre domaine se situe ? Vous pouvez réaliser gratuitement un Quickscan sur **guardian360.fr/quickscan**.

2.2 Jeu de données

Le benchmark repose sur 12 914 domaines analysés avec succès au cours de cette période de mesure. Tous les domaines sont pris en compte dans le benchmark global. Pour la comparaison par pays, nous mettons en avant les quatre marchés clés de Guardian360. L'attribution à un pays se fait selon le code pays dans le domaine de premier niveau.

Segment	Nombre de domaines	Score moyen	Médiane
Pays-Bas (.nl)	4 278	68,9	65
Belgique (.be)	609	72,7	75
Allemagne (.de)	2 887	68,4	65
France (.fr)	215	64,3	65
Autres extensions de domaine	4 925	68,3	65
Tous les pays (total)	**12 914**	**68,6**	**65**

Tableau 1. Taille et score moyen par segment.

La ligne « Autres extensions de domaine » regroupe les 4 925 domaines avec une extension différente ou générique, comme .com, .eu, .ch et .net. Ces domaines sont pris en compte dans le benchmark global mais ne constituent pas un pays distinct mis en avant, car l'extension n'est pas un indicateur fiable du pays d'origine. Ensemble, ils permettent au benchmark global de refléter une vue de marché large.

2.3 Ce que mesure le Quickscan

Le Quickscan évalue plusieurs catégories qui, ensemble, donnent une bonne image de l'hygiène de sécurité d'un site web :

- En-têtes de sécurité : HTTP Strict Transport Security (HSTS), X-Content-Type-Options et X-Frame-Options.
- Content Security Policy (CSP) : la présence d'une politique empêchant le chargement de contenus indésirables.
- Erreurs de configuration : entre autres l'absence de redirection HTTPS, la fuite d'informations techniques via les en-têtes X-Powered-By et Server, une page PHPinfo exposée et une méthode HTTP TRACE active.
- DNS : la présence et la validité d'un enregistrement SPF pour prévenir l'usurpation d'e-mail.
- SSL/TLS : l'utilisation de protocoles obsolètes, de chiffrements faibles et de vulnérabilités connues dans la connexion chiffrée.

3. Niveau de sécurité global

Le score Quickscan moyen sur l'ensemble des 12 914 domaines est de 68,6 points, avec une médiane de 65. Autrement dit, un domaine type satisfait aux principales exigences de base mais laisse une marge d'amélioration sur plusieurs points.

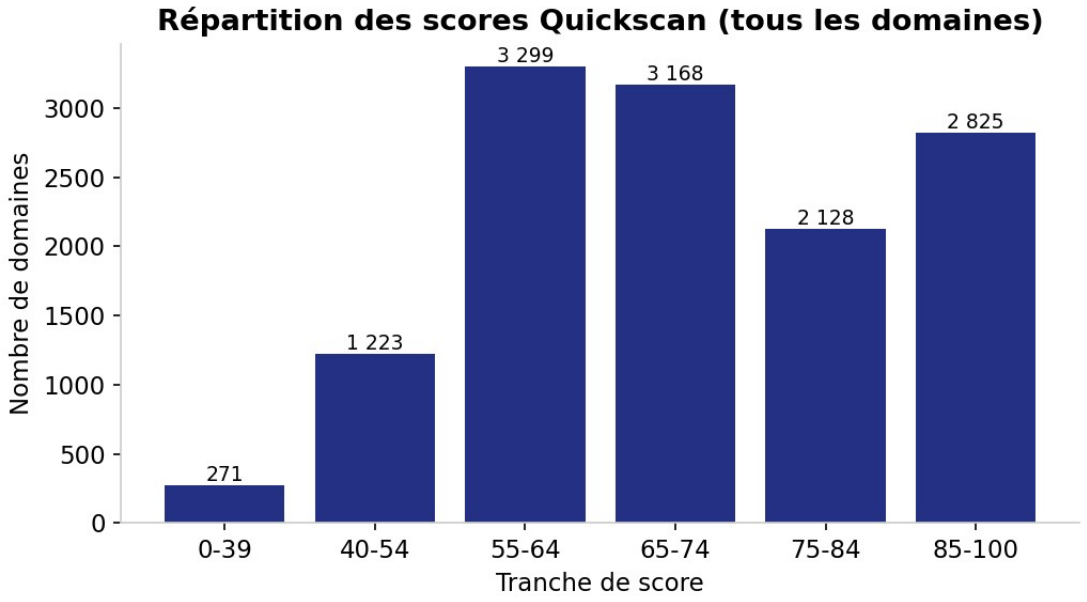

Figure 1. Répartition des scores Quickscan sur l'ensemble des domaines.

La répartition montre que le centre de gravité se situe dans la tranche intermédiaire. Les groupes les plus nombreux se situent entre 55 et 74 points. Dans le haut du classement, un groupe important de 2 825 domaines atteint un score de 85 ou plus, ce qui montre qu'un niveau de sécurité élevé est tout à fait atteignable. Dans le bas, un groupe plus restreint mais significatif de 271 domaines obtient moins de 40 points. Ces domaines cumulent généralement les lacunes et méritent la priorité.

4. Comparaison entre pays

Bien que les pays soient proches en score moyen, des différences significatives apparaissent sur certains aspects. La figure ci-dessous présente le score moyen par pays, comparé au benchmark global.

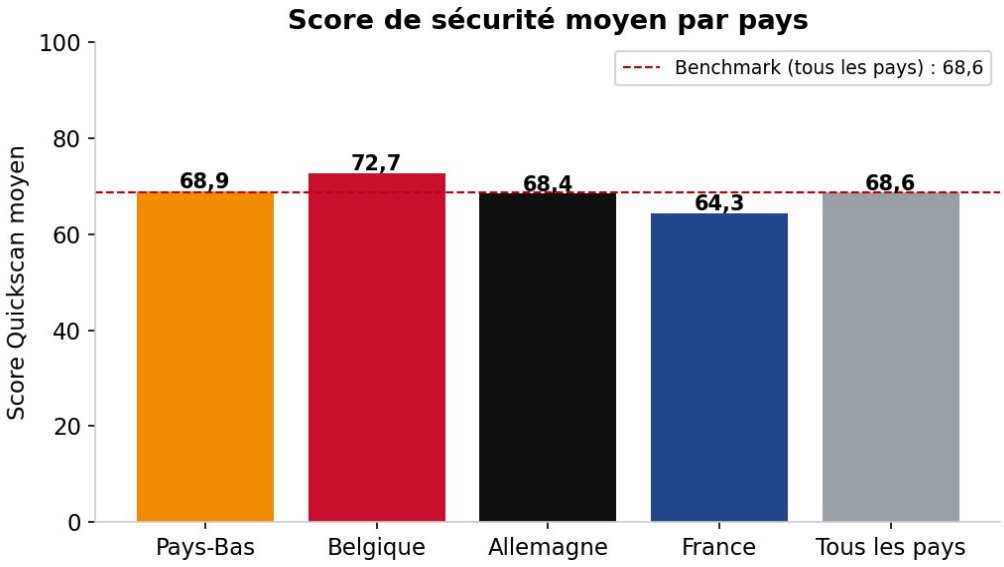

Figure 2. Score de sécurité moyen par pays par rapport au benchmark.

La Belgique se distingue positivement. Le score moyen de 72,7 comme la médiane de 75 se situent nettement au-dessus du benchmark. Les Pays-Bas et l'Allemagne suivent la moyenne presque exactement. La France est la plus en retrait à 64,3, même si l'échantillon français, avec 215 domaines, est plus petit et donc plus sensible aux valeurs extrêmes.

La figure suivante concrétise les différences par thème. Elle indique le pourcentage de domaines par pays sur lesquels la vulnérabilité concernée a été détectée. Une valeur plus faible est préférable.

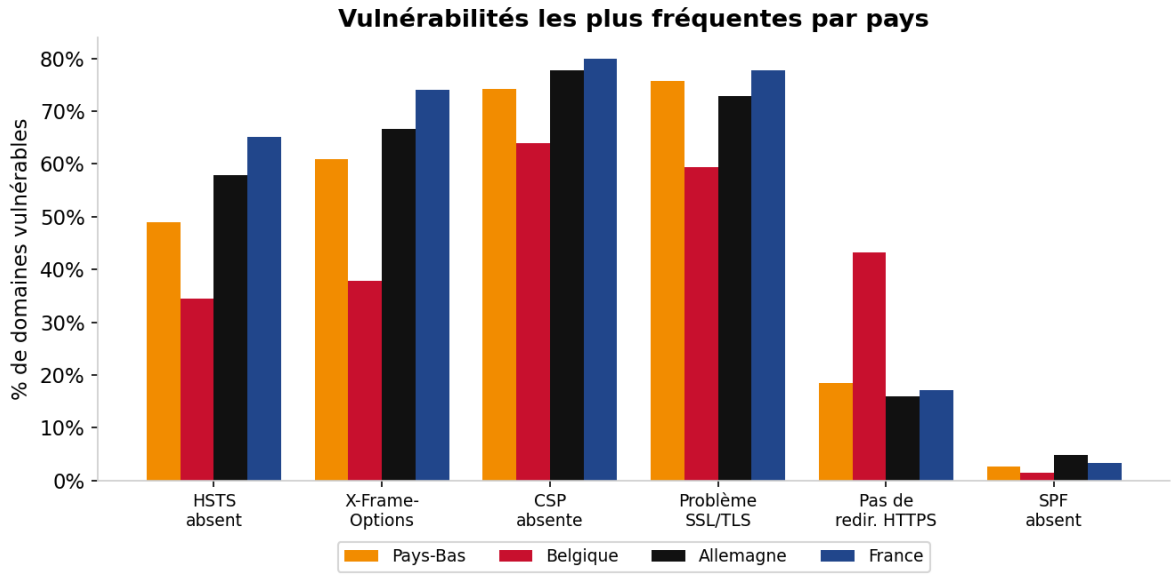

Figure 3. Pourcentage de domaines vulnérables par pays pour les principaux thèmes.

Le constat confirme la position forte de la Belgique sur les en-têtes de sécurité et sur le SSL/TLS. Fait notable, la Belgique est moins bonne sur la redirection HTTPS : 43,3% des domaines belges n'orientent pas

automatiquement les visiteurs vers une connexion chiffrée. La France affiche les taux les plus élevés d'en-têtes manquants, tandis que l'Allemagne divulgue relativement souvent des informations techniques via l'en-tête Server et présente le plus souvent un enregistrement SPF absent ou faible.

5. Constats par thème

Le tableau ci-dessous présente la ventilation complète des pourcentages de vulnérabilité par thème et par pays. Tous les pourcentages correspondent à la part des domaines sur lesquels la lacune a été détectée. Pour chaque thème, une valeur plus faible est préférable.

Thème	NL	BE	DE	FR	Total
HSTS absent ou faible	48,9%	34,5%	57,9%	65,1%	49,9%
X-Content-Type-Options absent	54,1%	33,5%	57,6%	67,9%	53,7%
X-Frame-Options absent	60,9%	37,8%	66,7%	74,0%	60,4%
Content-Security-Policy absente	74,3%	64,0%	77,7%	80,0%	73,2%
Pas de redirection HTTPS	18,4%	43,3%	16,0%	17,2%	19,7%
X-Powered-By révèle la technologie	31,9%	9,7%	23,5%	35,3%	25,5%
En-tête Server révèle la version	3,2%	2,5%	9,4%	7,9%	5,4%
PHPinfo exposé	1,3%	0,2%	2,6%	1,4%	1,6%
HTTP TRACE actif	0,9%	0,5%	1,2%	1,9%	0,9%
SPF absent ou faible	2,7%	1,5%	4,9%	3,3%	4,3%
Vulnérabilité SSL/TLS	75,7%	59,4%	72,9%	77,7%	75,6%

Tableau 2. Pourcentage de domaines vulnérables par thème et par pays.

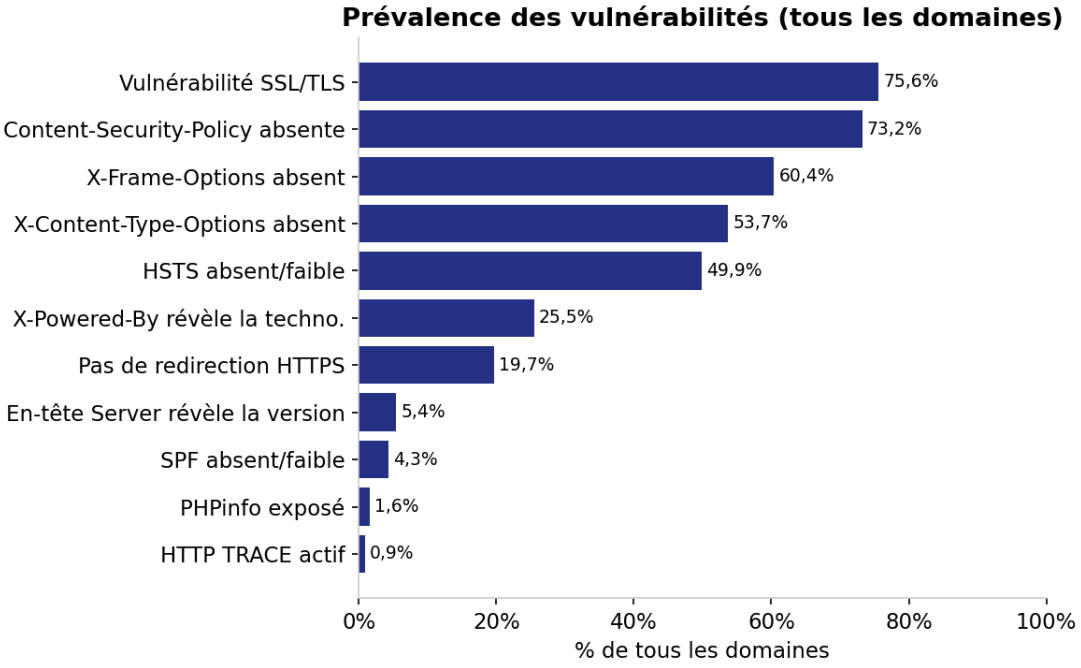

Figure 4. Prévalence des vulnérabilités sur l'ensemble des domaines, par ordre croissant.

5.1 En-têtes de sécurité

Les en-têtes de sécurité sont un moyen peu coûteux et efficace de contrer une grande partie des attaques courantes. Ils restent pourtant largement absents. Sur 60,4% des domaines, un en-tête X-Frame-Options est

absent, ce qui rend le site vulnérable au clickjacking. Sur près de la moitié, une configuration HSTS correcte fait défaut et sur 53,7% l'en-tête X-Content-Type-Options. La Belgique fait nettement mieux sur les trois en-têtes, tandis que la France affiche systématiquement les pourcentages les plus élevés.

5.2 Content Security Policy

La Content Security Policy est la lacune la plus fréquente de ce benchmark. Sur 73,2% des domaines, une CSP est totalement absente. Une CSP bien configurée est l'une des mesures les plus efficaces contre le cross-site scripting et l'injection de contenus indésirables. Si cette mesure est si souvent absente, c'est qu'une CSP doit être soigneusement adaptée au site et se trouve donc souvent reportée. Là encore, la Belgique fait le mieux à 64,0% et la France le moins bien à 80,0%.

5.3 Erreurs de configuration

Les erreurs de configuration les plus graves sont heureusement rares. Une page PHPinfo exposée n'a été trouvée que sur 1,6% des domaines et une méthode HTTP TRACE active sur 0,9%. La fuite d'informations techniques est plus tenace. Sur 25,5% des domaines, l'en-tête X-Powered-By révèle la technologie utilisée, ce qui aide les attaquants à rechercher des vulnérabilités de manière ciblée. La redirection HTTPS mérite une attention particulière en Belgique, où 43,3% des domaines n'ont pas cette mesure de base.

5.4 SPF et sécurité de la messagerie

L'enregistrement SPF empêche des acteurs malveillants d'envoyer facilement des e-mails au nom d'un domaine. Sur l'ensemble des domaines, un enregistrement SPF correct est absent sur 4,3%. C'est relativement faible, ce qui indique que le SPF est désormais largement adopté. L'Allemagne fait un peu moins bien ici, à 4,9%.

5.5 Configuration SSL/TLS

La connexion chiffrée est présente presque partout, mais sa qualité laisse à désirer. Sur 75,6% de l'ensemble des domaines, au moins une vulnérabilité SSL/TLS a été détectée, comme la prise en charge de protocoles obsolètes tels que TLS 1.0 ou la proposition de chiffrements faibles. Avec l'absence de CSP, c'est la lacune la plus fréquente. La Belgique limite les dégâts à 59,4%, tandis que la France affiche le pourcentage le plus élevé, à 77,7%.

6. Conclusions et recommandations

Le benchmark dépeint un marché où les fondamentaux sont largement en place, mais où les mesures de sécurité préventives à forte valeur accusent un retard structurel. Quatre conclusions se dégagent.

1. Le niveau de base est correct, sans plus. Avec un score moyen de 68,6 et une médiane de 65, le marché se situe dans la moyenne. Le large groupe de domaines entre 55 et 74 points montre qu'un effort limité permet de gagner beaucoup.

2. Les en-têtes, la CSP et le TLS sont les plus grandes opportunités. Ces trois thèmes présentent les taux de vulnérabilité les plus élevés tout en étant relativement faciles à améliorer. Ils constituent donc le point de départ logique de tout programme d'amélioration.

3. Les différences entre pays sont nettes. La Belgique est en tête, la France en retrait, et les Pays-Bas et l'Allemagne suivent le benchmark. Ces différences offrent des angles pour un développement commercial ciblé par pays.

4. Le Quickscan rend la progression mesurable. Comme chaque domaine reçoit un score clair et une liste concrète de constats, l'amélioration peut être rendue visible immédiatement. Cela fait du Quickscan un outil solide, tant pour un premier contact que pour un suivi périodique.

6.1 Recommandations pour les MSP, partenaires et distributeurs

- Positionnez le Quickscan comme une mesure de référence gratuite qui permet à un client (potentiel) de voir immédiatement comment son domaine se situe par rapport à ce benchmark.
- Utilisez les différences entre pays de ce rapport pour un développement commercial ciblé, par exemple en mettant l'accent sur les en-têtes de sécurité manquants en France.
- Proposez le Quickscan comme service récurrent, afin que les clients puissent mesurer leur progression périodiquement et rendre les améliorations visibles.

6.2 Recommandations pour les organisations

- Déterminez votre propre position de départ par rapport à ce benchmark à l'aide d'un Quickscan.
- Concentrez la première étape d'amélioration sur les en-têtes de sécurité et la redirection HTTPS, car ils sont rapides à mettre en œuvre et à faible impact.
- Planifiez une deuxième étape autour de la Content Security Policy et du durcissement TLS, là où se trouvent les gains les plus importants sur le fond.
- Répétez l'analyse périodiquement afin que la progression reste visible et que le niveau de sécurité soit maintenu.

Réaliser vous-même un Quickscan ?

Vous voulez savoir comment votre domaine se situe par rapport à ce benchmark ? Réalisez gratuitement un Quickscan sur

guardian360.fr/quickscan

Annexe. Précisions méthodologiques

Les chiffres de ce rapport sont issus des résultats bruts du Guardian360 Quickscan. Seules les analyses ayant le statut « completed » ont été retenues. Les analyses échouées ou incomplètes ont été exclues. Pour cette édition, cela concerne 717 analyses échouées sur un total de 13 631, laissant 12 914 résultats exploitables.

L'attribution à un pays se fait selon le code pays du domaine de premier niveau. Un domaine se terminant par .nl est attribué aux Pays-Bas, .be à la Belgique, .de à l'Allemagne et .fr à la France. Cette méthode est simple et reproductible, mais comporte une limite. Une organisation active dans un pays donné mais utilisant un domaine générique comme .com n'est pas attribuée à ce pays. Ces domaines sont pris en compte dans le benchmark global.

Une vulnérabilité est comptabilisée lorsque le Quickscan marque l'élément concerné comme vulnérable. Pour le SSL/TLS, un domaine est signalé comme vulnérable dès qu'au moins un constat individuel, comme un protocole obsolète ou un chiffrement faible, est détecté. Les pourcentages indiqués représentent toujours la part des domaines au sein du segment concerné.